REMARKS

Claims 2-11 were pending and examined. In the Office Action, Claims 2-11 were rejected under 35 U.S.C. §§112, second paragraph, 102(b) and 103(a), no claims were objected to and no claims were allowed. The rejection of Claims 2-11 has been made final.

By this Amendment and Reply, Claims 7, 9 and 11 are proposed to be amended, no claims are proposed to be canceled and Claims 12-17 are proposed to be added. Accordingly, Claims 2-17 are presented for further examination. Entry of the above-described amendments and favorable reconsideration of this application in light of the following discussion is respectfully requested.

Proposed Amendments to Claims:

As noted above, it is proposed to amend Claims 7, 9 and 11. Support for the proposed claim amendments may be found in the original disclosure. Thus, no new matter is presented. Appendix A, attached hereto and incorporated by reference herein to this Amendment and Reply, provides a detailed illustration of the present invention and supporting portions of the Specification.

Additionally, as part of this Amendment and Reply, it is proposed to add Claims 12-17. Support for these newly added claims may be found in the original disclosure and, thus, no new matter is presented.

Examiner's Response to Previously Submitted Arguments:

In the Office Action the Examiner states that Applicant's arguments submitted 08 April 2005 directed to then pending Claims 2-11 were considered but found non-persuasive. Accordingly, the Examiner maintains, and now makes final, the rejection of Claims 2-7 and 11 under 35 U.S.C. §102(b) as allegedly being anticipated by Deo et al. (U.S. Patent No. 6,496,928), Claims 2-7, 9 and 11 under 35 U.S.C. §102(b) as allegedly being anticipated by Hoffmann et al. (U.S. Patent No. 5,608,800), Claim 8 under 35 U.S.C. §103(a) as allegedly being unpatentable over Hoffmann et al. in view of Horstmann (U.S. Patent No. 6,009,410), Claim 10 under 35 U.S.C. §103(a) as allegedly being unpatentable over Hoffmann et al. in view of Official Notice, and Claims 2-8 and 11 under 35 U.S.C. §112, second paragraph, as being indefinite for allegedly failing to particularly point out and distinctly claim the subject matter that Applicant regards as the invention.

Rejection under 35 U.S.C. §112, Second Paragraph:

With respect to the rejection of Claims 2-8 and 11 under 35 U.S.C. §112, second paragraph, Applicant proposes amending Claim 11 to replace a term "initializing" by a term "storing." Support for the proposed amendment may bc found in the original disclosurc and at least at page 3, lines 20-31 and FIG. 1. Thus, no new matter is presented.

It is respectfully submitted that one skilled in the art at the time of the invention would appreciate that a secure memory 11 of a control center 10 and a corrcsponding memory 11' of a receiver 30 each store a secret, main key.

In view of the foregoing, the Examiner is respectfully requested to enter the proposed amendment to Claim 11 and to reconsider and withdraw the rejection of Claims 2-8 and 11 under 35 U.S.C. §112, second paragraph.

Prior Art Rejections:

As noted above, the Examiner maintains, and now makes final, the rejection of Claims 2-7 and 11 under 35 U.S.C. §102(b) as allegedly being anticipated by Deo et al. This rejection is respectfully disagreed with, and traversed below.

The arguments and remarks made previously are repeated and incorporated by reference herein and, in particular, the descriptions of Deo et al., Hoffmann et al., and Horstmann.

As previously noted, Deo et al. merely disclose a systcm including a contcnt providcr 12, a wireless carrier 14, a computer 16 and a mobile device 18 (FIG. 1). The content provider 12 provides suitable data from a database. The data can be transmitted from the content provider 12 to the wireless carrier 14 to the mobile devicc 18; from thc content provider 12 to a computer 16 to the mobile device 18; and directly from the content provider 12 to the mobile device 18. See Deo et al. at Col. 1, lines 66 and 67, Col. 2, lines 1-67, and Col. 6 lines 18 – 26. The content provider 12 and the wirelcss carrier are configured to program the mobile device 18 with an encryption key for decrypting a content message. See Deo et al. at Col. 22, lines 57 – 60.

Deo et al. describe that an encrypted content message must bc dccryptcd for usc by a mobile device (e.g., a receiver). See Deo et al. Col. 27, lines 42-45 and Col. 28, lines 1-31.

The present invention, as recited in the claims as now written, teaches and claims, determining a sequence number (e.g., by extracting the sequence number from the received message (Claims 2 and 12) or producing it from an initial value of a pseudo-random number generator (Claims 5 and 13)); forming a check key from the determined sequence number; and verifying the received message by forming a calculated signature and comparing the calculated signature to the signature received in the message. See independent Claim 11, as now proposed to be written. Support for the proposed amendment to Claim 11 may be found in the original disclosure and at least at page 5, line 23 to page 6, line 29 and FIG. 1. Thus, no new matter is presented.

For example, independent Claim 11, as now written, recites:

> "11. A method for signing a message from a sender and for checking a signature at a receiver, the method comprising the steps of:
>
> storing, in a control center and a receiver, a shared main key;
>
> causing the control center to produce one or more sequence numbers;
>
> using a selected one of the sequence numbers and the shared main key to create a signing key by means of a one-time encryption;
>
> providing at least one pair of the signing key and the selected sequence number to the sender via a secure transmission;
>
> the sender using the at least one pair of the signing key and the selected sequence number to form a signature for a message;
>
> the sender forming a data set;
>
> the sender sending the message to the receiver via the data set containing at least the message and the signature;
>
> determining, at the receiver, a sequence number for the received data set;
>
> passing the determined sequence number and the shared main key through a one-time encryption to produce a check key;
>
> using the check key and the determined sequence number to form a calculated signature; and
>
> comparing the calculated signature to the received signature to verify the received message."

As such, the present invention teaches and claims calculating a signature for each message received at a receiver, and comparing the calculated signature to a signature attached to a message by a sender, rather than decrypting one or more portions of a received message to determine a signature assigned by the sender (Deo et al.). Therefore, Deo et al. can not anticipate independent Claim 11, as it is well settled that "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

Since independent Claim 11, as now written, is deemed patentable over Deo et al., Claims 2-7, which depend from and further limit Claim 11, are patentable.

In view of the above, the Examiner is respectfully requested to reconsider and withdraw the rejection of Claims 2-7 and 11, as now proposed to be written, under 35 U.S.C. §102(b) as being anticipated by Deo et al.

The Examiner maintains, and now makes final, the rejection of Claims 2-7, 9 and 11 under 35 U.S.C. §102(b) as allegedly being anticipated by Hoffmann et al. This rejection is respectfully disagreed with, and traversed below.

As previously noted, Hoffmann et al. merely disclose a means for transmitting useful data from a transmitter to a receiver. The transmitter comprises useful data, a signature associated with the useful data, and a transfer key. The receiver contains a corresponding transfer key. The transfer key permits confidential transmission of random data. In order to safeguard the transmission of the useful data, the signature associated with the useful data is converted to an enciphered signature. A message transmitted from the transmitter to the receiver comprises coupling data, enciphered random data, the useful data and the enciphered signature.

Hoffmann et al. also disclose checking the transmitted message through a series of enciphering and deciphering steps including, for example, recovering the random data by deciphering the enciphered random data with the aid of the transfer key (Hoffmann et al. at Col. 3, lines 65-67); determining a symmetric key using one-way enciphering of the calculated random data and the coupling data (Hoffmann et al. at Col. 4, lines 1-3); and recovering the signature for the received message by deciphering the enciphered signature with the aid of the determined symmetric key (Hoffmann et al. at Col. 4, lines 4-5). Once recovered, the signature is checked and if errors are revealed the message is rejected.

As noted above, the present invention teaches and claims calculating a signature for each message received at a receiver, and comparing the calculated signature to a signature attached to a message by a sender, rather than performing one or more enciphering and deciphering steps of portions of a received message to recover a signature assigned by a sender and determine whether the signature is correct (Hoffmann et al.). Therefore, Hoffmann et al. can not anticipate independent Claim 11, as now proposed to be written.

Moreover, independent Claim 9 is proposed to be amended to include a similar limitation as is found in Claim 11. Therefore, Hoffmann et al. can not anticipate independent Claim 9, as now proposed to be written.

Since independent Claims 9 and 11, as now written, are deemed patentable over Hoffmann et al., Claims 2-7, which depend from and further these claims, are also deemed patentable.

In view of the above, the Examiner is respectfully requested to reconsider and withdraw the rejection of Claims 2-7, 9 and 11, as now proposed to be written, under 35 U.S.C. §102(b) as being anticipated by Hoffmann et al.

The Examiner maintains, and now makes final, the rejection of Claim 8 under 35 U.S.C. §103(a) as allegedly being unpatentable over Hoffmann et al. in view of Horstmann et al. This rejection is respectfully disagreed with, and traversed below.

The deficiencies of Hoffmann et al. with respect to independent Claim 11 are outlined above.

The Examiner notes that Hoffmann et al. do not explicitly teach the receiver maintaining a list of already used sequence numbers and rejecting messages including already used sequence numbers. Rather, the Examiner proposes combination of Hoffmann et al. with Horstmann et al., which disclose a licensing clearinghouse that maintains a list of already used tickets (Horstmann et al. at Col. 5, lines 21-27).

Assuming, arguendo, that these documents were somehow combined, it is respectfully submitted that the proposed combination of Hoffmann et al. and Horstmann et al. would merely disclose a means for transmitting a message from a transmitter to a receiver, the message including coupling data, enciphered random data, the useful data and the enciphered signature and, at the receiver, checking the transmitted message through a series of enciphering and deciphering steps including recovering the random data by deciphering the enciphered random data with the aid of the transfer key; determining a symmetric key using one-way enciphering of the calculated random data and the coupling data; recovering the signature for the received message by deciphering the enciphered signature with the aid of the determined symmetric key; and once recovered, the signature is checked and if errors are revealed the message is rejected (Hoffmann et al.). Where, in accordance with Horstmann et al., one or more of the previously used symmetric keys E, random data Z or coupling data K (it not being clear which of these items the Examiner asserts is a sequence number), are stored in a list and presumably used within the enciphering and/or deciphering steps.

Therefore, even if these documents were somehow combined, the proposed combination is still not seen to expressly or implicitly describe or suggest, the present invention as recited in Claims 11 and 8, as now written, where a signature for each message received at a receiver is calculated, and compared to a signature attached to a message by a sender, and wherein the receiver stores a list of previously used sequence numbers.

In view of the above, the Examiner is respectfully requested to reconsider and withdraw the rejection of Claim 8 under 35 U.S.C. §103(a) as allegedly being unpatentable over Hoffmann et al. in view of Horstmann et al.

The Examiner maintains, and now makes final, the rejection of Claim 10 under 35 U.S.C. §103(a) as allegedly being unpatentable over Hoffmann et al. in view of Official Notice. This rejection is respectfully disagreed with, and traversed below.

The deficiencies of Hoffmann et al. with respect to independent Claim 9 are outlined above.

Assuming, arguendo, that it is old and well known practice to use deterministic methods to produce numbers, as is asserted by the Examiner, it is respectfully submitted that the proposed combination of Hoffmann et al. and Official Notice of the use of deterministic methods is still not seen to expressly or implicitly describe or suggest, the present invention as recited in Claims 9 and 10 where a device for signing a message which is sent from a sender to a receiver comprises, for example, a signature checker provided in the receiver having inputs connected to the message and to the signature of the received data message block, and wherein the inputs of the signature checker are connected to an output of a second one-time encrypter for providing a check key, whose inputs are connected to the second memory of the receiver for the secret main key and to a means for determining a sequence number for the received data message block, the check key and the determined sequence number being used to form a calculated signature for comparison to the signature of the data message block, as recited in independent Claim 9, as now proposed to be written.

Therefore, even if the proposed combination is somehow made, it is still not seen to expressly or implicitly describe or suggest, the present invention as recited in Claims 9 and 10, as now written

In view of the above, the Examiner is respectfully requested to reconsider and withdraw the rejection of Claim 10 under 35 U.S.C. §103(a) as allegedly being unpatentable over Hoffmann et al. in view of Official Notice.

Applicant believes that the foregoing amendments and remarks are fully responsive to the Office Action and that the claims herein are allowable. In view of the foregoing points that distinguish Applicant's invention from those of the prior art and render Applicant's invention novel and non-obvious, Applicant respectfully requests that the Examiner reconsider the present application, remove the rejections, and allow the application to issue.

If the Examiner believes that a telephone conference with Applicant's attorneys would be advantageous to the disposition of this case, the Examiner is invited to telephone the undersigned.

Based on the foregoing and for at least these reasons, Applicant respectfully submits that claims of the application in question are in condition for allowance and an early action to that effect is earnestly solicited.

No fee is believed due with the filing of this Amendment and Reply. However, if a fee is due, Applicant authorizes the payment of any additional charges that may be necessary to maintain the pendency of the present application to the undersigned attorney's Deposit Account No. 503342.

Respectfully submitted,

By____________________
Richard R. Michaud
Registration No. 40,088
Attorney for Applicant

Michaud-Duffy Group LLP
CenterPoint
306 Industrial Park Road
Suite 206
Middletown, CT 06457-1532
(860) 632-7200